REMARKS

Claims 1-26 are pending in the Application.

Claims 1-13, 15 and 18-26 stand rejected.

Claims 14 and 16-17 have been objected to.

I. INFORMATION DISCLOSURE STATEMENT

The Examiner has requested that Applicant submit in an IDS the "Trusted Computing Platform Alliance" incorporated by reference on page 1 of the Specification. Applicant does not consider the Trusted Computing Platform Alliance to be prior art. Furthermore, the Trusted Computing Platform Alliance is a consortium of computer processor manufacturers to arrive at acceptable standards for trusted computing systems. The Examiner may view more information about the Trusted Computing Platform Alliance by visiting the web site www.trustedcomputing.org. As a courtesy to the Examiner, Applicant has submitted in the enclosed information disclosure statement one of the documents referenced at that web site, the Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile.

II. REJECTION UNDER 35 U.S.C. § 112

Claim 26 stands rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Applicant respectfully traverses the Examiner's rejection. The claims as originally filed in this Application are also part of the original disclosure of the invention. In other words, claim 26 provides support for itself in that regard. Furthermore, one skilled in the art would understand what is meant by "the use authorization in the non-migratable storage tree is obtained by hashing the concatenation of the user authorization in the migratable storage tree with a fixed string."

III. REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-13, 15 and 18-26 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Microsoft Corporation "Microsoft Windows 2000 Public Key Infrastructure" as updated April 1999 (hereinafter referred to as "Microsoft"). Applicant respectfully traverses this rejection. As the Examiner is well aware, for a claim to be anticipated under § 102, each and every element of the claim must be found within the cited prior art reference. As Applicant will hereinafter assert, the Examiner has not sufficiently showed where in Microsoft the various limitations of the claims are found. Though an Examiner may give claim language a broad interpretation, such an interpretation must be reasonable, and also consistent with the interpretation that those skilled in the art would reach, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in Applicant's Specification. MPEP § 2111.

The claims in the Application recite migratable and non-migratable storage trees. Applicant respectfully asserts that the Examiner has completely ignored these claim limitations, and has in no way found such limitations in the cited reference. A migratable key can be transferred to other trusted platform modules chips, while non-migratable keys cannot be transferred. Specification, page 8, lines 16-17. Thus, such non-migratable keys are locked to the hardware, which is the only hardware that can decrypt such keys. Specification, page 8, lines 17-19.

With respect to claims 1 and 18, the Examiner has asserted that page 3, paragraphs 3-6 of Microsoft teaches the claim limitations in claims 1 and 18. Applicant respectfully traverses. The Microsoft reference merely describes private key cryptography. There is absolutely no teaching, expressly or inherently, or suggestion within Microsoft of migratable and non-migratable storage trees. These paragraphs in Microsoft merely describe the use of private and public keys for the secure transmission of information, and the use of certificates for authenticating public keys. Nothing within Microsoft teaches creating a migratable storage tree with a storage root key. Nothing within Microsoft teaches creating a non-migratable storage tree with the storage root key, wherein the migratable storage tree and the non-migratable storage tree are identically structured. The Examiner has made no attempt at identifying any language within Microsoft that teaches migratable and non-migratable storage trees.

Furthermore, with respect to claim 18, the Examiner has completely ignored the additional limitations within that claim that the migratable storage tree and the non-migratable storage tree are identically structured with corresponding keys and authentication data. For this reason alone, the Examiner has failed to prove a *prima facie* case of anticipation in rejecting claim 18.

Claims 2 and 19 recite that the migratable storage tree and the non-migratable storage tree are created by a trusted computing module in accordance with the Trusted Computing Platform Alliance. The Examiner has attempted to reject these claims by citing all of page 6 of Microsoft. Nowhere within Microsoft, and specifically page 6, is the Trusted Computing Platform Alliance discussed in any way. This page merely describes certificate hierarchies. Furthermore, there is absolutely no disclosure of a trusted computing module. Likewise, there is absolutely no discussion of migratable and non-migratable storage trees.

With respect to claims 3 and 20, these claims recite that the migratable storage tree comprises migratable keys and a user key, wherein the non-migratable storage tree comprises non-migratable keys and a user key. The Examiner has attempted to reject these claims by citing page 3, paragraphs 3-6 and the discussion of certificate hierarchies of page 6 of Microsoft. As asserted above, nowhere within Microsoft is there a discussion of migratable and non-migratable storage trees. Furthermore, nowhere within Microsoft are migratable and non-migratable keys discussed.

With respect to claims 4 and 22, these claims recite that the non-migratable storage tree will include non-migratable storage keys corresponding to each migratable storage key in the migratable storage tree. In rejecting these claims, the Examiner has recited page 8 of Microsoft, and specifically the section on Generating Keys. This section merely discusses the generation and management of keys for use in PK technology. There's absolutely no teaching or inference of non-migratable storage trees having non-migratable storage keys corresponding to migratable storage keys in a migratable storage tree.

With respect to claims 5 and 24, these claims recite that use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree. The Examiner has attempted to reject these claims by referring to page 12 of the Microsoft reference. All this language in the smart card logon section discloses is that the enablement of a smart card

logon creates a more secure access than a password-based logon. There is nothing within this language that teaches use authorization in the non-migratable storage tree will be identical to use authorization in the migratable storage tree.

Claim 6 recites the further steps of requesting a migratable storage tree and requesting a non-migratable storage key. Since Microsoft does not in any way teach or discuss migratable and non-migratable storage keys, claim 6 is not anticipated by Microsoft. Certificate enrollment is not the same as requesting migratable and non-migratable storage keys.

Claim 7 recites that the step of requesting a migratable storage key will identify a parent key in the migratable storage tree, and the step of requesting a non-migratable storage key will identify a parent key in the non-migratable storage tree that corresponds to the parent key in the migratable storage tree. The Examiner again cites the certificate enrollment section on page 12 of Microsoft. This language does not in any way teach or suggest migratable and non-migratable storage keys. Furthermore, there is nothing within this language that teaches or suggests that a parent key is identified in the migratable storage tree and that a parent key is identified in the non-migratable storage tree that corresponds to the parent key in the migratable storage tree.

Claim 8 recites the step of when a key loading request is made for a migratable storage key, loading a key from the non-migratable storage tree instead of loading a corresponding key from the migratable storage tree. The Examiner has attempted to reject these claim limitations by citing page 5, paragraph 3 of Microsoft. In this language, there is no teaching of a key loading request. There is no language teaching migratable and non-migratable storage trees. There is no teaching of loading a key from the non-migratable storage tree instead of loading a corresponding key from the migratable storage tree.

Claim 9 is an independent claim that recites limitations that are significantly different than those recited in claim 1. However, the Examiner has rejected claim 9 by merely referencing the Examiner's rejection for claim 1. This is wholly inappropriate, and completely fails to prove a *prima facie* case of anticipation in rejecting claim 9. Nevertheless, Applicants incorporate their traversal of the rejection of claim 1 in responding to the rejection of claim 9. Yet still further, Microsoft does not teach or suggest splitting a request to create a new migratable storage key with given authentication data and a first parent key into first and second commands. Microsoft does not teach or suggest wherein the first command creates a migratable storage key with the

given authentication data and the first parent key. Microsoft does not teach or suggest wherein the second command request creating a non-migratable storage key with the given authentication data and a second parent key which is determined from looking up a key that corresponds to the first parent key in a database.

Claim 10 recites wherein the migratable storage key and the non-migratable storage key are associated in a database. The Examiner has cited page 2 of Microsoft, and specifically the section on Public Key Functionality. This language does not in any way teach or suggest migratable and non-migratable storage keys. There is no reference to a database in this language. Public and private keys are not migratable and non-migratable storage keys.

Claim 11 recites that the non-migratable key is a multi-prime key. A shared secrets key is not a multi-prime key. A shared secrets key is not a non-migratable key.

Claim 12 recites that the non-migratable key is an elliptic curve key. Page 2, paragraph 2 of Microsoft does not teach a non-migratable key being an elliptic curve key. The reference to Elliptic Curve Cryptography does not teach that a non-migratable is an elliptic curve key. The Examiner has again ignored the limitation "non-migratable."

With respect to claim 13, the digital signatures section on page 2 of Microsoft does not teach creating a new migratable signing key with the given authentication data and a third parent key. There is absolutely no reference to a migratable signing key. Page 5, paragraph 3 does not in any way recite storing the new migratable signing key with the given authentication data and the third parent key. Page 4, paragraph 2 does not in any way teach or suggest storing the new migratable signing key with the given authentication data and a fourth parent key where the fourth parent key is a non-migratable key associated with the third parent key in a database. The Examiner is ignoring the claim limitations.

With respect to claim 15, the Examiner has again ignored the limitation "non-migratable."

With respect to claim 21, the section on Secret Key Agreement via Public Key does not teach or suggest that the migratable storage tree comprises migratable keys and encrypted user data wherein the non-migratable storage tree comprises non-migratable keys and encrypted user data.

With respect to claim 23, the first paragraph on page 16 of Microsoft mentions PKIX subsets. These are not the same as the non-migratable storage tree including non-migratable storage keys corresponding to a subset of the migratable storage keys in the migratable storage tree.

Microsoft does not teach the limitations of claim 25 that the use authorization in the non-migratable storage tree can be deduced from user authorization in the migratable storage tree with additional data.

IV. CONCLUSION

As a result of the foregoing, it is asserted by Applicants that the remaining Claims in the Application are in condition for allowance, and respectfully request an early allowance of such Claims.

Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining problems.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicants

By: _____
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851

AUSTIN_1\247881\1
7036-P173US 04/13/2004